1. A method of detecting vulnerabilities in source code comprising:

   generating a model which describes certain characteristics about the actions to be performed in a routine, and

   using the model in conjunction with pre-specified criteria for the corresponding routine to determine whether the routine possesses vulnerabilities which could enable actions in the routine to be performed outside of the intended design.

2. The method of claim 1 wherein the vulnerabilities are privilege escalations.

3. The method of claim 1 wherein the pre-specified criteria for the corresponding routine includes rules about the semantic behavior of the routine.

4. A system for detecting vulnerabilities in source code comprising:

   computed implemented logic for generating a model which describes certain characteristics about the actions to be performed in a routine, and

   computed implemented logic for using the model in conjunction with pre-specified criteria for the corresponding routine to determine whether the routine possesses vulnerabilities which could enable actions in the routine to be performed outside of the intended design.

5. The system of claim 4 wherein the computed implemented logic for using the model in conjunction with pre-specified criteria for the corresponding routine to determine whether the routine possesses vulnerabilities which could enable actions in the routine to be performed outside of the intended design includes a database specifying rules to detect vulnerabilities based on an analysis of the models.